

UNITED STATES DISTRICT COURT
for the
District of Oregon

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))
A black Apple iPhone, as described in Attachment A)
)
)
)
Case No. 3:20-mc-00453

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

A black Apple iPhone, as described in Attachment A hereto,

located in the _____ District of Oregon _____, there is now concealed (*identify the person or describe the property to be seized*):

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
21 U.S.C. § 841(a)(1) and 846	Possession with the Intent to Distribute and Conspiracy to Possess with the Intent to Distribute Methamphetamine; Use of a Communication Facility
21 U.S.C. § 846(b)	

The application is based on these facts:

See affidavit which is attached hereto and incorporated herein by this reference.

Continued on the attached sheet.

Delayed notice of _____ days (*give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Anthony Burke, TFO, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephone at 10:17 a.m. (specify reliable electronic means). *[Signature]*

Date: 05/13/2020

City and state: Portland, Oregon

Hon. Stacie F. Beckerman, United States Magistrate Judge

Printed name and title

DISTRICT OF OREGON, ss: AFFIDAVIT OF ANTHONY BURKE

**Affidavit in Support of an Application Under Rule 41
for a Warrant to Search and Seize Evidence Including Digital Evidence**

I, Anthony Burke, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, Section 2510(7). I am currently employed as a Detective with the Salem Police Department (Salem, Oregon) and have approximately 5 years of law enforcement experience. I am also a sworn Task Force Officer (“TFO”) with the Federal Bureau of Investigations (“FBI”), and assigned to the Resident Office in Salem, Oregon. I have been a TFO since February 2020. I am authorized, and presently assigned, to investigate violations of the Comprehensive Drug Abuse Prevention and Control Act of 1970, Title 21, United States Code, et seq., and other violations of federal law.

2. I have received training through the Department of Public Safety Standards and Training (DPSST) in the State of Oregon, for the certification as a police officer in the State of Oregon and I hold an Intermediate Certificate through this institution. I have had all stages of police training, including crime investigation, acquisition and preservation of evidence, felony apprehension, search and seizure, and other police operations. During my law enforcement career, I have participated in hundreds of drug related investigations and search warrants. I have personally utilized all means available to law enforcement during the course of an investigation, which includes but is not limited to: surveillance, informants, undercover officers, video

surveillance, photography, pen registers, vehicle trackers, wire taps, search warrants, body wires and other physical and technological investigative means.

3. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of a black iPhone (hereinafter, **McGuire Phone**), currently in law enforcement custody at the Salem Police Department at 555 Liberty Street Southeast, Salem, Oregon, as described in Attachment A hereto, and the extraction of electronically stored information from the Phone, as described in Attachment B hereto. As set forth below, I have probable cause to believe and do believe that **McGuire Phone** contains evidence, fruits, and instrumentalities, as set forth in Attachment B hereto, of violations of Title 21, United States Code, Sections 841(a)(1), 841(b)(1)(A), 843(b) and 846.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

5. Title 21, U.S.C., Sections 841(a)(1) and 846, Possession with the Intent to Distribute and Conspiracy to Possess with the Intent to Distribute, make it unlawful to possess with the intent to distribute controlled substances, and to conspire to do so. Title 21, U.S.C.,

Section 843(b), Use of a Communication Facility, makes it unlawful to use a communication facility in furtherance of a drug crime.

Statement of Probable Cause

6. During the course of an investigation that began in April of 2020 Joshua McGuire (hereinafter referred to as “MCGUIRE”) was identified as distributing methamphetamine in the Salem, Oregon area. During the course of the investigation, several controlled buys from MCGUIRE by a cooperating defendant (hereinafter referred to as “CD-1”) were conducted. The controlled buys would occur when CD-1, at law enforcement direction, would send a text message to MCGUIRE and they would arrange to meet for the purpose of purchasing methamphetamine.

Description of Cooperating Defendant 1 (CD-1)

7. CD-1 provided information in attempt to obtain consideration for their pending criminal charges in the State of Oregon. No threats or promises have been made to CD-1 in hopes of gaining his/her cooperation. CD-1 is a convicted felon. CD-1’s criminal history consists of eight (8) arrest cycles, including an unlawful possession of methamphetamine conviction (2008) and a theft in the first degree conviction (2007).

First Controlled Buy

8. In April of 2020, at my direction, CD-1 contacted MCGUIRE via text message for the purposes of purchasing methamphetamine from MCGUIRE. During this conversation, MCGUIRE agreed to meet CD-1 at his storage unit on Turner Road Southeast, which I knew to be in the 4000 Block of Turner Road Southeast, Salem, Oregon. During the text message exchange between CD-1 and MCGUIRE, which I observed, CD-1 asked MCGUIRE if he had “something small” that CD-1 could “get for myself.” I asked CD-1 what he/she meant by

“something small” and CD-1 stated this meant that he/she was requesting an amount of methamphetamine that was for their own personal use.

9. I conducted a search of CD-1’s person and vehicle to ensure CD-1 had no money, weapons or controlled substances on CD-1’s person prior to sending CD-1 to meet with MCGUIRE. I provided CD-1 with one hundred and fifty dollars of United States currency and told CD-1 to purchase one half ounce of methamphetamine. At the conclusion of the controlled purchase of methamphetamine, CD-1 returned to me an amount of methamphetamine that was consistent with what I had requested CD-1 to purchase and provided me twenty-five dollars of United States currency and stated one half ounce cost one hundred and twenty-five dollars. This is consistent with prices for methamphetamine within the Willamette Valley region. I later field tested the suspected methamphetamine that was provided to me by CD-1 and it field tested presumptive positive for the presence of methamphetamine. This controlled buy was audio recorded.

Second Controlled Buy

10. Later in April of 2020, at my direction, CD-1 contacted MCGUIRE via text message for the purpose of purchasing methamphetamine from MCGUIRE. During the text conversation, I observed MCGUIRE to say “I’ve got some O’s if you need some or if you just want to smoke.” Based on my training and experience, I know “O’s” to be an abbreviated term for “ounces” which is a measurement used when speaking in terms of quantity of controlled substances. During the text conversation, I observed CD-1 state that he/she would be in contact with MCGUIRE shortly. During the conversation, MCGUIRE indicated that he was working on

his vehicle in his shop. I believe that he refers to his storage unit on Turner Road Southeast in Salem, Oregon as his shop based on information that CD-1 has provided me.

11. A search of CD-1's person and vehicle was conducted prior to sending CD-1 to 4000 Turner Road Southeast to conduct the controlled buy to ensure CD-1 had no controlled substances, weapons or United States currency. Once it was determined CD-1 did not possess any of these items, CD-1 was sent to 4000 Turner Road Southeast with four hundred and seventy-five dollars in United States currency and was instructed to purchase two (2) ounces of methamphetamine from MCGUIRE. CD-1 then traveled over to 4000 Turner Road Southeast to purchase the methamphetamine.

12. During the controlled buy, I was able to monitor audio between CD-1 and MCGUIRE. I could hear when the purchase was complete and followed CD-1 to a pre-determined location where CD-1 provided me with what appeared to be two (2) ounces of methamphetamine. I later weighed the suspected methamphetamine, which weighed approximately two (2) ounces with packaging. I field tested the suspected methamphetamine and it field tested presumptive positive for the presence of methamphetamine.

Third controlled buy

13. During May of 2020, at my direction, CD-1 contacted MCGUIRE through text message to facilitate a transaction for methamphetamine. I witnessed the text conversation between CD-1 and MCGUIRE where MCGUIRE directed CD-1 to meet him at 4000 Turner Road Southeast.

14. Prior to CD-1 meeting with MCGUIRE, I met with CD-1 at an undisclosed location to ensure CD-1 did not possess any controlled substances, United States currency or weapons.

After checking CD-1 for the aforementioned items, I sent CD-1 with an audio recording device to 4000 Turner Road Southeast number “C8” to purchase one thousand dollars’ worth of methamphetamine.

15. At the completion of the controlled purchase of methamphetamine, CD-1 met me at an undisclosed location where he/she provided me with two hundred and twenty-eight grams of a crystal substance which appeared consistent with methamphetamine. I conducted a second check of CD-1’s person for controlled substances, United States currency and weapons and found none. I field tested the contents of the suspected methamphetamine, which field tested presumptive positive for the presence of methamphetamine.

16. The investigation, which included the above controlled buys from MCGUIRE, also included witness statements relating to MCGUIRE and law enforcement surveillance related to MCGUIRE.

17. On May 7, 2020, Hon. Youlee Yim You, United States Magistrate Judge, District of Oregon, signed search warrants 20-MC-441 A-C authorizing the government to search MCGUIRE’s residence at 1614 Chemeketa Street Northeast, Salem, Oregon 97301 (hereinafter referred to as “Residence”), MCGUIRE’s Dodge Ram 2500, Oregon License Plate Number 845DDH (hereinafter referred to as “Vehicle”), and MCGUIRE’s storage unit located at 4000 Turner Road Southeast, Salem, Oregon 97317 (hereinafter referred to as “Unit”).

18. On May 7, 2020 Investigators with SCU and the Federal Bureau of Investigation (FBI) executed the search warrant on MCGUIRE’s Unit, where the controlled buys occurred during the course of the investigation. MCGUIRE would refer to the storage unit as his “shop” where he also kept a vehicle at that he would work on. In their search of the Unit, investigators

seized three thousand, three hundred and ninety-four (3,394) grams of a suspected methamphetamine, which field tested presumptive positive for the presence of methamphetamine. Investigators also located a black Sig Sauer handgun with an obliterated serial number. I know this firearm to have been manufactured outside the state of Oregon. Also located in MCGUIRE's Unit were digital scales and packaging material.

19. On the same date, investigators executed the search warrant on MCGUIRE's Residence. Prior to the execution of the search warrant, MCGUIRE was detained by officers at his Residence. Following advisement of his *Miranda* rights, he made a statement to officers inferring that they were going to find a bunch of cash. In their subsequent search of MCGUIRE's Residence, where he is the sole occupant, investigators seized three hundred and ninety-five (395) grams of suspected methamphetamine, which field tested presumptive positive for the presence of methamphetamine. An additional seven (7) firearms that I know to have been manufactured outside the state of Oregon were also seized from the Residence, along with approximately \$400,000.00 in United States currency.

20. I reviewed MCGUIRE's criminal history and know that he was previously convicted of the felony of Unlawful Delivery of Methamphetamine in Polk County Circuit Court (Case Number 17CR00343) and was sentenced to 18 months in prison, and thereby prohibited from possessing a firearm.

//

//

//

//



Items seized from MCGUIRE's Residence and Unit on May 7, 2020

21. MCGUIRE was taken in to custody for possession of methamphetamine with intent to distribute and felon in possession of a firearm. When MCGUIRE was taken in to custody, law enforcement seized a black iPhone (**McGuire Phone**) which was in MCGUIRE's right front pant pocket. Also in his pocket was approximately forty-seven (47) grams of a crystal substance, which based on my training and experience appeared consistent with methamphetamine.

22. Based on the previous controlled purchases of methamphetamine from MCGUIRE, I know that MCGUIRE uses his phone to coordinate the trafficking of illegal drugs.

23. I know from my training and experience that drug traffickers and others involved in illegal activity use cellphones, applications, and other portable technology to facilitate and advance their illegal endeavors. Furthermore, I know that information contained on cellular devices can provide significant investigative intelligence value into criminal offenses, and co-conspirators.

24. **McGuire Phone** is currently stored at the Salem Police Department at 555 Liberty Street Southeast, Salem, Oregon. In my training and experience, I know that the Phone has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Phone first came into the possession of the Salem Police Department.

25. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet,¹ including the use of apps.² Wireless telephones may also include a global positioning system (“GPS”) technology for determining the location of the device.

¹ The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

² Apps is an abbreviation for applications. An app is a self-contained program or piece of software designed to fulfill a particular purpose. An app can run on the Internet, on a computer, on a cell phone, or on other electronic devices.

26. Based on my training, experience, and research, I know that **McGuire Phone** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device and a personal assistant, or PDA. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

27. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the Phone because, based on my knowledge, training, and experience, I know:

a. Phones can store information for long periods of time, including information viewed via the Internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person “deletes” a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, the Phone may contain electronic

evidence of how it has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

d. Data on the Phone can provide evidence of a file that was once on the Phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on the Phone that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the Phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times the Phone was in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

f. A person with appropriate familiarity with how the Phone works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the Phone was used, the purpose of its use, who used it, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data

that can be merely reviewed by a review team and passed along to investigators. Whether data stored on the Phone is evidence may depend on other information stored on the Phone and the application of knowledge about how a Phone functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how the Phone was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the Phone.

28. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Phone consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Phone and computer-assisted scans and searches of the entire Phone that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

29. The initial examination of the Phone will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

30. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phone or image do not contain any data falling within the

scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

31. If an examination is conducted, and it is determined that the Phone does not contain any data falling within the ambit of the warrant, the government will return the Phone to its owner within a reasonable period of time following the search and will seal any image of the Phone, absent further authorization from the Court.

32. The government may retain the Phone as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phone and/or the data contained therein.

33. The government will retain a forensic image of the Phone for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

34. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

35. Based on the foregoing, I have probable cause to believe, and I do believe, that **McGuire Phone**, as described in Attachment A, contains evidence, fruits, and instrumentalities, of violations of Title 21, United States Code, Sections 841(a)(1), 841(b)(1)(A), 843(b) and 846, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the **McGuire Phone** described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

By Phone

Anthony Burke
Task Force Officer
Federal Bureau of Investigations

Sworn in before me in accordance with the requirements of Fed. R. Crim. P. 4.1 by
10:17 a.m.
telephone at p.m. on May 13, 2020.


HONORABLE STACIE F. BECKERMAN
United States Magistrate Judge

ATTACHMENT A

Phone to Be Searched

The phone to be searched is a black iPhone found in MCGUIRE's right front pocket when taking in to custody and is currently located on the premises of 555 Liberty Street Southeast, Salem, Oregon.



Attachment A

ATTACHMENT B

Items to Be Seized

1. All records on the Device described in Attachment A that relate to violations of Title 21, U.S.C., Sections 841(a)(1) and 846, Possession with the Intent to Distribute a Controlled Substance and Conspiracy to Possess with the Intent to Distribute a Controlled Substance and Title 21, U.S.C., Section 843(b), Use of a Communication Facility to Distribute a Controlled Substance (hereinafter collectively “Target Offenses”) and involve Joshua MCGUIRE (“MCGUIRE”) since December 1, 2019, including:
 - a. Communication between the Device and others regarding drug transactions, drug storage locations, and movement of money derived from the sale of drugs.
 - b. Lists of customers and related identifying information.
 - c. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions.
 - d. Information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information).
 - e. Information recording MCGUIRE’s schedule or travel from December 1, 2019 to the present.
 - f. Bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

4. The examination of the Device may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

5. The initial examination of the Device will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

6. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Device or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without

authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Device does not contain any data falling within the ambit of the warrant, the government will return the Device to its owner within a reasonable period of time following the search and will seal any image of the Device, absent further authorization from the Court.

9. The government may retain the Device as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Device and/or the data contained therein.

10. The government will retain a forensic image of the Device for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.